

METHOD AND APPARATUS FOR LOW DENSITY PARITY CHECK ENCODING OF DATA

5

Background of the Invention

1. Technical Field

10 The present invention generally relates to a method and apparatus for low-density parity-check (LDPC) encoding of data and particularly relates to block encoding of data based on a parity check matrix for mapping the data into LDPC code words for binary and multilevel modulation for data communication and for recording systems.

2. Description of Related Art

15 In Gallager: "Low-density parity-check codes, Cambridge, MA, MIT Press 1963.", it is shown that, based on message-passing decoders, it is possible to come extremely close to the channel capacity of the binary-input additive white Gaussian noise channel (AWGN). Since then, it has been shown that LDPC codes can come very close to capacity on many practical communication and recording channels. Therefore, LDPC codes have been considered as an alternative to turbo codes. Specifically, LDPC codes exhibit a better asymptotic performance than turbo codes, they are less affected by error floors, and offer a variety of tradeoffs between decoder complexity and performance. An advantage of LDPC codes is the low implementation complexity of the sum-product algorithm that is used to decode them. Simplified versions of the sum-product
20 algorithm drive complexity lower with negligible loss in decoding performance as compared to full sum-product decoding.
25

30 In many magnetic recording applications such as hard-disk drives or tape systems, information is stored in binary form. In these applications, inner modulation codes concatenated with outer Reed-Solomon codes are employed to provide reliable extraction of the written information. Turbo and LDPC codes may push the areal density of magnetic recording systems to the limit for

presently available magnetic components. It has been shown that, despite present sector-size constraints of hard-disk drives limiting the block length of a code and the high code-rate requirement, simple iterative decoding schemes can bring performance within approximately 1.5 dB of the theoretical limit. This represents a significant gain compared to existing systems.

5 High-rate LDPC codes appear to have advantages over convolutional or turbo codes when used as outer codes in a magnetic recording system. For example, LDPC codes do not seem to suffer from error floors at error rates of 10^{-8} . Furthermore, the sparseness of the parity-check matrix of LDPC codes results in decoding algorithms that are less complex compared to serially concatenated systems with convolutional outer codes. Also, no interleaver is needed between the LDPC encoder
10 and the channel, because interleaving can be implicitly incorporated into the LDPC code. The potential gains of LDPC codes over the traditional Reed-Solomon codes for the magnetic recording channel have been presented in, T. Mittelholzer, A. Dholakia, and E. Eleftheriou
"Reduced-Complexity Iterative Decoding of Low Density Parity Check Codes for Generalized
Partial Response Channels," *IEEE Trans. Magn.*, 37(2), pp. 721-728, March 2001. In magnetic
15 storage systems LDPC codes are expected to push the areal density to its ultimate limit.

In many communication systems, including both wired and wireless transmission systems, there are strict limitations on transmit signal bandwidth. Such limitations impose a demand for signal modulation with a number of levels greater than two. Many conventional systems employ
20 Trellis-coded modulation (TCM) in such applications. However, a problem associated with TCM is that it is unsuitable for iterative decoding. Therefore, further improvements in signal quality at an acceptable complexity are difficult to achieve.

"A turbo TCM scheme with low decoding complexity," Catena Networks Inc., Temporary
25 Document BI-090, ITU-T Study Group 15, Question 4, Goa, India, 23-27 Oct. 2000, "Proposal of decision making for turbo coding and report of performance evaluation of proposed
TTCM(PCCC) with R-S code and without R-S code," Mitsubishi Electric Corp., Temporary Document BI-003, ITU-T Study Group 15, Goa, India, 23-27 Oct. 2000, and "Results of the
requirements requested in the coding ad hoc report," Vocal Technologies Inc., Temporary
30 Document HC-073, ITU-T Study Group 15, Question 4, Huntsville, Canada, 31 July - 4 August

2000, describe turbo-coding schemes for multilevel ADSL and VDSL transmission. These turbo-coding techniques involve encoding of the information bits by parallel concatenation of convolutional encoders in recursive systematic form and iterative decoding by one of several possible turbo-decoding techniques. "Block product turbo codes for G.dmt.bis and G.lite.bis,"
 5 Globespan Inc., Temporary Document BA-063, ITU-T Study Group 15, Question 4, Antwerp, Belgium, 19-23 June 2000 describes the application of block product codes using component Bose-Chaudhuri-Hocquenghem (BCH) codes and their soft iterative decoding based on the Chase algorithm. These techniques offer some performance enhancements over Trellis coding at the expense of incurring additional complexity.

10

Application development relating to the alternative coding technique of LDPC codes, as described in R. G. Gallager, "Low-density parity-check codes," IRE Trans. Info. Theory, vol. IT-8, pp. 21-28, Jan. 1962, D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes, Electron. Lett., vol. 32, no. 18, pp. 1645-1646, Aug. 1996, D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," IEEE Trans. on Inform. Theory, vol. 45, No. 2, pp. 399-431, Mar. 1999, and FOSSORIER, M.P.C., MIHALJEVIC, M., and IMAI, H.: "Reduced complexity iterative decoding of low density parity check codes based on belief propagation", IEEE Trans. Commun., 1999, 47, (5), pp. 673-680 ,
 15 has to date focussed on applications requiring binary modulation such as wireless systems or digital magnetic recording. LDPC codes can also, however, be applied to multilevel transmission.

20

K. R. Narayanan and J. Li, "Bandwidth efficient low density parity check coding using multilevel coding and iterative multistage decoding," Proc. Int. Symp. on Turbo-Codes, Brest, France, pp. 165-168, Sept. 2000 describes a multilevel coding technique based on binary LDPC block codes.
 25 This technique uses LDPC block codes for bit-interleaved modulation or for multilevel coding with iterative multi-stage decoding. For bit-interleaved LDPC modulation according to this technique, all the bits used to select a multilevel symbol are LDPC code bits. For multilevel coding, several LDPC block codes are used as component codes in a multilevel scheme. This

technique has the drawback of requiring more than one LDPC encoder/decoder, leading to substantial implementation complexity especially for long codes and/or large constellation sizes.

"Low density parity check coded modulation for ADSL," Aware Inc., Temporary Document

5 BI-081, ITU-T Study Group 15, Question 4, Goa, India, 23-27 October 2000 also describes a multilevel coding technique based on binary LDPC block codes. This technique is similar to TCM, except that LDPC coding is employed instead of convolutional coding. In particular, set partitioning follows the same principle as that used in TCM. This technique has the drawback of requiring an additional Bose-Chaudhuri-Hoeguenhem (BCH) code which adds to system
10 complexity. Also, set partitioning, as required in TCM and similar schemes, leads to poor performance for soft-decision based decoding techniques.

Temporary Document RN-25, ITU Telecommunications Standardization Sector, Study Group 15, New Jersey, USA, 21-25 May 2001 describes a deterministic LDPC methodology and its applications to ADSL and ADSL Lite transmission. The methodology proposed therein requires a precomputation of the a generator matrix using, for example, Gaussian elimination. The encoding requires $O(N^2)$ operations.

Co-pending IBM patent application ^{number 10/045,810} ~~reference CH9-2000-0087~~ describes a method for multilevel data communication comprising: dividing a set of information bits to be transmitted into a first group and a second group; encoding the first group to generate a block code ; selecting a subset of symbols in a constellation of symbols in dependence on the block code according to a Gray-coded mapping function; selecting a symbol within the subset in dependence on the second group according to a Gray-coded mapping function; and, transmitting the selected symbol. This
25 method offers superior performance in terms of achievable coding gains. The coding gains arise because block coding schemes can be decoded iteratively, thereby leading to substantial performance gains as compared to trellis-coded modulation. Particularly preferred embodiments of this method comprise multilevel encoding schemes based on LDPC codes or simple product codes that do not need interleaving and that can be decoded via the simple sum-product
30 algorithm (SPA) or low-complexity derivatives thereof.

A disadvantage associated with LDPC codes is that they demand relatively high encoding complexity. When an LDPC code word is obtained by multiplying the information block with the generator matrix of the code, encoding requires $O(N^2)$ operations, where N is the length of the code. Such an encoding procedure is not "linear in time." Furthermore, there is a preprocessing step needed to compute the generator matrix of the code from the specified LDPC parity-check matrix. The computation of the generator matrix involves Gaussian elimination, which requires $O(N^3)$ operations. Even though the preprocessing can be performed once for a particular LDPC check matrix and can be carried out off line, the computation cost can be prohibitive when decoding for applications requiring selection of one of a family of parity check matrices. This is the case, for example, in XDSL where the code is selected on a per connection basis. The topic of efficient encoding for LDPC codes has been addressed in L. Ping, W. K. Leung, and N. Phamdo, "Low density parity check codes with semi-random parity check matrix," *Electron. Letters*, Vol. 35, No. 1, pp. 38-39, 7th Jan. 1999; D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Trans. on Communications*, Vol. 47, No. 10, pp. 1449-1454, Oct. 1999 ; and, R. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. on Information Theory*, Vol. 47., No. 2, pp.638-656, Feb. 2001.

In L. Ping, W. K. Leung, and N. Phamdo, "Low density parity check codes with semi-random parity check matrix," *Electron. Letters*, Vol. 35, No. 1, pp. 38-39, 7th Jan. 1999, the parity-check matrix of the LDPC code is "semi-random" in the sense that it includes a deterministic and a random part. The deterministic part is in a band-diagonal or "zigzag" form to allow efficient encoding. The rest of the parity-check matrix is created randomly by avoiding 4-cycles. In D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Trans. on Communications*, Vol. 47, No. 10, pp. 1449-1454, Oct. 1999 and R. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. on Information Theory*, Vol. 47., No. 2, pp.638-656, Feb. 2001 , the parity-check matrix is again generated by a random construction and a triangular or "approximate triangular" form is

imposed to allow efficient encoding. These constructions each lead to linear-time encodable LDPC codes. However, they have a number of drawbacks, including:

- (a) Randomly constructed parity-check codes cannot be specified via a small number of parameters. In other words, all the positions of the nonzero elements of the parity-check matrix must be individually given;
- (b) preprocessing is sometimes required to bring the parity-check matrix into triangular or approximate triangular form; and,
- (c) the codes obtained result in loss in performance as compared with randomly constructed LDPC codes.

It would be desirable to provide parity-check matrices that lead to LDPC codes having linear-time encoding complexity. It would also be desirable to provide parity-check matrices that are fully deterministic and can be specified via a small number of parameters. It would also be desirable to provide parity-check matrices that require a minimum amount of, or no, preprocessing.

Summary of the Invention

In accordance with the present invention, there is now provided a method for low-density parity-check (LDPC) encoding of data, the method comprising: defining a first $M \times N$ parity check matrix representative of the low density parity check code; generating, based on the first parity check matrix, a second parity check matrix having an $M \times M$ triangular sub-matrix; and, mapping the data into an LDPC code word based on the second parity check matrix.

The method may further comprise eliminating 4-cycles from the second matrix. Alternatively, the defining of the parity check matrix may comprise cyclically shifting of rows of the first matrix to eliminate 4-cycles from the outset. Preferred embodiments of the present invention comprise setting entries along the main diagonal of the $M \times M$ triangular sub-matrix to the same value.

Viewing the present invention from another aspect, there is now provided apparatus for low-density parity-check (LDPC) encoding of data, the apparatus comprising: matrix definition logic for defining a first $M \times N$ parity check matrix; a triangular matrix generator for generating a second parity check matrix based on the first parity check matrix; the second parity check matrix having an $M \times M$ triangular sub-matrix; and, an encoder for mapping the data into an LDPC code word based on the second parity check matrix.

Viewing the present invention from yet another aspect, there is now provided a computer program product for low-density parity-check (LDPC) encoding of data, the computer program product comprising a machine readable storage medium storing computer program code which, when loaded in a programmable data processor, configures the processor to perform the steps of: defining a first $M \times N$ parity check; generating, based on the first parity check matrix, a second parity check matrix having an $M \times M$ triangular sub-matrix; and, mapping the data into an LDPC code word based on the second parity check matrix.

The present invention also extends to a data transmitter for transmitting data received from an information source via a communications channel, the data being encoded by the transmitter into a low-density parity-check (LDPC) code word, the transmitter comprising: matrix definition logic for defining a first $M \times N$ parity check; a triangular matrix generator for generating a second parity check matrix based on the first parity check matrix; the second parity check matrix having an $M \times M$ triangular sub-matrix; and, an encoder for mapping the data into an LDPC code word based on the second parity check matrix.

The present invention further extends to a data storage system for storing data received from an information source in a data storage channel, the data being encoded by the system into a low-density parity-check (LDPC) code word, the system comprising: matrix definition logic for defining a first $M \times N$ parity check matrix; a triangular matrix generator for generating a second parity check matrix based on the first parity check matrix; the second parity check matrix having an $M \times M$ triangular sub-matrix; and, an encoder for mapping the data into an LDPC code word based on the second parity check matrix.

Parity-check matrices thus provided lead to LDPC codes having linear-time encoding complexity. Such matrices are fully deterministic and can be specified via a small number of parameters. Also, such matrices require a minimum amount of, or no, preprocessing. The performance of the obtained codes is as good as or better than the randomly constructed LDPC codes.

5

Preferred embodiments of the present invention to be described shortly utilise parity-check matrix constructions for so-called "array codes". Array codes are described by M. Blaum, P. Farrell, and H. van Tilborg, "Array codes," in Handbook of Coding Theory, V.S. Pless and W.C. Huffman Eds., Elsevier 1998. The direct application of array-code constructions to obtain LDPC parity-check matrices are described in J. L. Fan, "Array codes as low-density parity-check codes," Proc. Int. Symp. on Turbo Codes, Brest, France, pp. 543-546, Sept. 2000, and E. Eleftheriou and S. Oelcer, "LDPC codes for G.dmt.bis and G.lite.bis," International Telecommunication Union, ITU-T, Study Group 15 / Question 4, Temporary Document CF-060, Clearwater, FL, 8-12 Jan. 2001. Although the codes in the last mentioned two references are specified via a small number of parameters, they are not linear-time encodable.

10

15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

Brief Description of the Drawings

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

20

Figure 1 is a block diagram of a communications system;

Figure 2 is a block diagram of a transmitter for the communications system;

25

Figure 3 is a block diagram of another transmitter for the communications system;

Figure 4 is a block diagram of an matrix generator for the transmitter;

30

Figure 5 is a flow chart corresponding to an encoder function of the transmitter

Figure 6 is a flow chart corresponding to the matrix generator; and

Figure 7 is another flow chart corresponding to the matrix generator;

5 Figure 8 is a block diagram of a data storage system; and,

Figure 9 is a block diagram of another example of a transmitter for the communications system.

Detailed Description of Illustrative Embodiment

10

Referring first to Figure 1, a preferred embodiment of the present invention comprises a transmitter 10 for connection to a receiver (not shown) via a communication channel 20 such a Digital Subscriber Line (DSL) communications channel. In operation, the transmitter 10 receives a sequence of information bits 30 from an information source 40 such as a computer system, mobile telephone, fixed line telephone, or similar data communications endpoint. The transmitter 10 converts the information bits 30 into symbols 50 for transmission to the receiver via the channel 20.

15
20
25
30

Referring now to Figure 2, in a particularly preferred embodiment of the present invention, the transmitter 10 comprises a divider 100, a block encoder 110 connected to the divider 110 and a symbol mapper 120 connected to the block encoder 110 and the divider 100. A parity check matrix generator 160 is connected to the encoder 110. In operation, at each modulation instant, the divider 100 divides a set of information bits 30 from the information source 40 to be communicated into a first group 130 and a second group 140. The block encoder 110 encodes the second group 140 to generate a block code 150 based on a parity check matrix provided by the matrix generator. The parity check matrix is generated by the matrix generator based on code parameters 170. The symbol mapper 120 selects a subset of symbols in a constellation of symbols in dependence on the block code 150 according to a Gray-coded mapping function. The symbol mapper 120 also selects a symbol within the subset in dependence on the first group 130 according to a Gray-coded mapping function. The selected Symbol 50 is then communicated to

the receiver via the channel 20. The divider 100 may implemented by a shift register or similar logical function. It will be appreciated that the transmitter 10 may be implemented by hardwired logic, by a general purpose processor or dedicated digital signal processor programmed with computer program code, or by a combination of hardwired logic and computer program code.

5

Referring now to Figure 3, in a modification to the transmitter 10 herein before described with reference to Figure 2, the divider 100 is omitted and the block encoder 110 encodes all the information bits 30 received from the information source 40 to generate the block code 150. The symbol mapper 120 selects a symbol in a constellation of symbols in dependence on the block code 150 according to a Gray-coded mapping function. The selected symbol 50 is then communicated to the receiver via the channel 20.

10

With reference to Figures 4, in a preferred embodiments of the present invention, the matrix generator 160 comprises matrix definition logic 300 connected to a triangular matrix generator 310. With reference to Figure 5, in operation, at step 350, the matrix definition logic 300 defines a first $M \times N$ parity check matrix 320 based on input code parameters 170. At step 360, the triangular matrix generator 310 generates a second matrix based on the first matrix. The second matrix has an $M \times M$ triangular sub-matrix. At step 370, the second matrix is supplied from the matrix generator 160 to the encoder 110. Data input to the encoder 110 is then mapped LDPC code words based on the second matrix. Two approaches to definition of the parity check matrix and the generation of the triangular matrix in preferred embodiments of the present invention will now be described with reference to Figures 6 and 7.

15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

Referring to Figure 6, in a preferred embodiment of the present invention, matrix generation comprises three steps, 1, 2, and 3. In step 1, a matrix H is defined according to the definition of parity-check matrices for array codes. Step 2 is a triangularization step that deterministically modifies the matrix H to achieve an upper-triangular structure. Step 3 includes a simple procedure to eliminate 4-cycles that may have been introduced in the second step.

25

30 Step 1: Definition of H

The array-code like LDPC parity check matrix H is defined by three parameters: a prime number p and two integers k and j such that $k, j \leq p$. The matrix H has dimensions $jp \times kp$ and is given by

$$H = \begin{bmatrix} I & I & I & \cdots & I \\ I & a & a^2 & \cdots & a^{k-1} \\ I & a^2 & a^4 & \cdots & a^{2(k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I & a^{j-1} & a^{2(j-1)} & \cdots & a^{(j-1)(k-1)} \end{bmatrix},$$

where I is the $p \times p$ identity matrix and a is a $p \times p$ permutation matrix representing a single left or right cyclic shift. For example:

$$a = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{or} \quad a = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

The parameters j and k provide the column and row weight of H , respectively. By construction, the matrix H is 4-cycle free. In other words, there are no two rows that have overlapping ones in more than one position.

H represents the parity-check matrix of a family of LDPC codes with code word length $N = kp$ and number of parity checks $M = jp$. An LDPC code with code word length $N' < N$ or number of parity checks $M' < M$ is easily obtained by discarding the $N - N'$ rightmost columns and the $M - M'$ lowest rows of H . The resulting $M' \times N'$ matrix is then used instead of H in steps 2 and 3, with obvious modifications to the sizes of the matrices involved.

Step 2: Triangularization of H

Let H be represented in the block-matrix form

$$\mathbf{H} = \left[\mathbf{H}_1 \mid \mathbf{H}_2 \right]$$

where \mathbf{H}_1 has dimensions $jp \times jp$ and \mathbf{H}_2 has dimensions $jp \times (k-j)p$. Let \mathbf{U} be the $jp \times jp$ upper-triangular matrix obtained from \mathbf{H}_1 by replacing each element on the main diagonal of \mathbf{H}_1 with a 1 and by setting all the elements below the main diagonal to 0. The $jp \times kp$ matrix

$$\mathbf{H}_U = \left[\mathbf{U} \mid \mathbf{H}_2 \right]$$

defines the parity-check matrix of a linear-time encodable LDPC code.

Note that, although the matrix \mathbf{H} is 4-cycle free by construction, \mathbf{H}_U may not be free of 4-cycles due to the introduction of the upper triangular matrix \mathbf{U} . However, 4-cycles are easily detected and eliminated as demonstrated in the next step.

Step 3: Elimination of 4-cycles

Let $\mathbf{A} = \mathbf{H}_U \cdot \mathbf{H}_U^T$, where T denotes matrix transposition. The diagonal element $a_{m,m}$, $m = 1, \dots, jp$ of \mathbf{A} gives the Hamming weight of row m , i.e., the number of symbols checked by the parity-check m of matrix \mathbf{H}_U . The off-diagonal element $a_{m,n}$, $m, n = 1, \dots, jp$, $m \neq n$, gives the number of symbols checked by both parity-check m and parity-check n . In the absence of 4-cycles, $a_{m,n} \leq 1$.

Therefore, to ensure that the parity-check matrix is free of 4-cycles:

(a) Compute the lower-triangular part of $\mathbf{A} = \mathbf{H}_U \cdot \mathbf{H}_U^T$.

(b) If $a_{m,n} > 1$, ($m, n = 1, \dots, jp$; $m < n$), set the (n,m) -th element of \mathbf{H}_U equal to zero.

Denote by $\tilde{\mathbf{H}}_U$ the matrix that is obtained at the end of Step 3. The LDPC code defined by $\tilde{\mathbf{H}}_U$ has code word length $N = kp$, number of parity checks $M = jp$, and information block length $K = (k-j)p$. Linear-time encodability using $\tilde{\mathbf{H}}_U$ is shown in the next section.

- 5 Efficient encoding is achieved directly from the parity-check matrix $\tilde{\mathbf{H}}_U$ without the need to compute the generator matrix of the code. Recall that since LDPC codes are linear block codes, an N -tuple \mathbf{x} is an LDPC code word if and only if $\tilde{\mathbf{H}}_U \cdot \mathbf{x} = \mathbf{0}$, where $\mathbf{0}$ is the $M \times 1$ null vector. The vector \mathbf{x} may be expressed in the form

10
$$\mathbf{x} = \begin{bmatrix} \mathbf{p} \\ \mathbf{s} \end{bmatrix}$$

where the $jp \times 1$ vector \mathbf{p} represents the *parity* part and the $(k-j)p \times 1$ vector \mathbf{s} represents the *systematic* part of the code word \mathbf{x} . The jp parity bits in \mathbf{p} are obtained in a recursive manner by employing

15
$$\tilde{\mathbf{H}}_U \cdot \begin{bmatrix} \mathbf{p} \\ \mathbf{s} \end{bmatrix} = \mathbf{0}$$

and exploiting the upper-triangular form of $\tilde{\mathbf{H}}_U$. To demonstrate this, let both vectors \mathbf{p} and \mathbf{s} be split into $p \times 1$ sub-vectors

20
$$\mathbf{p} = \begin{bmatrix} \mathbf{p}_1 \\ \mathbf{p}_2 \\ \vdots \\ \mathbf{p}_j \end{bmatrix} \quad \text{and} \quad \mathbf{s} = \begin{bmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \\ \vdots \\ \mathbf{s}_{k-j} \end{bmatrix},$$

where $\mathbf{p}_i = \{p_{i,n}; n = 1, 2, \dots, p\}$, $i = 1, 2, \dots, j$ and $\mathbf{s}_i = \{s_{i,n}; n = 1, 2, \dots, p\}$, $i = 1, 2, \dots, k-j$. Then the elements of \mathbf{p}_m are obtained for $m = j, j-1, \dots, 1$ by the set of recursions

$$p_{m,p} = \sum_{\ell=m+1}^j p_{\ell,\dots} + \sum_{\ell=1}^{k-j} s_{\ell,\dots}$$

$$p_{m,p-1} = (p_{m,p}) + \sum_{\ell=m+1}^j p_{\ell,\dots} + \sum_{\ell=1}^{k-j} s_{\ell,\dots}$$

5

:

$$p_{m,1} = (p_{m,\dots}) + \sum_{\ell=m+1}^j p_{\ell,\dots} + \sum_{\ell=1}^{k-j} s_{\ell,\dots}$$

where the second sub-indices of $p_{\ell,\dots}$ and $s_{\ell,\dots}$, which depend on the particular values assumed by the power of the matrix a , have been omitted to avoid notational burden. The terms shown in parentheses may actually not be present, depending, again, on the particular values of the power of the matrix a .

The above encoding process thus takes advantage of the triangular structure of the parity-check matrix \tilde{H}_U as well as of its sparsity. It can be shown that encoding requires about

$$\frac{N}{2} \left[j(1+r) + \left(1 - \frac{4}{j}\right)(1-r) \right]$$

XOR operations, where r is the rate of the code.

Referring now to Figure 7, a modification to the approach herein before described with reference to Figure 6 comprises two steps, 1' and 2'. Steps 1' and 2' will now described in detail.

Step 1': Definition of H^S

A matrix H^S is defined by cyclically shifting, in a blockwise manner, the rows of the matrix H . The amount of cyclic shift for each block-row is such that the $jp \times jp$ leftmost subblock of H^S contains the identity matrix I along its diagonal:

$$H^S = \begin{bmatrix} I & I & I & \cdots & I & I & \cdots & I \\ \alpha^{k-1} & I & \alpha & \cdots & \alpha^{j-2} & \alpha^{j-1} & \cdots & \alpha^{k-2} \\ \alpha^{2(k-2)} & \alpha^{2(k-1)} & I & \cdots & \alpha^{2(j-3)} & \alpha^{2(j-2)} & \cdots & \alpha^{2(k-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ \alpha^{(j-1)(k-j+1)} & \alpha^{(j-1)(k-j+2)} & \cdots & \cdots & I & \alpha^{j-1} & \cdots & \alpha^{(j-1)(k-1)} \end{bmatrix}.$$

Since H^S has been obtained from H via cyclic shifts only, it has column and row weights given by j and k , respectively, and is free of 4-cycles.

5

Step 2': Triangularization of H^S

The matrix H^S is triangularized by replacing with zeros the lower-triangular elements of its $jp \times jp$ leftmost subblock. As a result, the matrix H_U^S is obtained:

$$H_U^S = \begin{bmatrix} I & I & I & \cdots & I & I & \cdots & I \\ O & I & \alpha & \cdots & \alpha^{j-2} & \alpha^{j-1} & \cdots & \alpha^{k-2} \\ O & O & I & \cdots & \alpha^{2(j-3)} & \alpha^{2(j-2)} & \cdots & \alpha^{2(k-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ O & O & \cdots & O & I & \alpha^{j-1} & \cdots & \alpha^{(j-1)(k-1)} \end{bmatrix},$$

where O is the $p \times p$ null matrix.

The LDPC code defined by H_U^S has code word length $N = kp$, number of parity checks $M = jp$, and information block length $K = (k-j)p$. Also, H_U^S is 4-cycle free. Clearly, LDPC codes defined by H_U^S are linear-time encodable.

An LDPC code with code word length $N' < N$ or number of parity checks $M' < M$ is easily obtained by discarding the $N - N'$ rightmost columns and the $M - M'$ lowest rows of H_U^S .

Efficient encoding is achieved in the same manner as herein before described with reference to the approach herein before described with reference to Figure 6. It can be shown to require

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
20

$$\frac{N}{2}[r(j+3) + (j-3)]$$

XOR operations, where r is the rate of the code.

- 5 The parity-check matrices obtained in the embodiments of the present invention herein before described with reference to Figures 6 and 7 have a triangular form. In references D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Trans. on Communications*, Vol. 47, No. 10, pp. 1449-1454, Oct. 1999 and R. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE*
 10 *Trans. on Information Theory*, Vol. 47., No. 2, pp.638-656, Feb. 2001, it is shown that fast encoding is also possible for LDPC codes having a parity-check matrix in "approximate triangular" form

$$\begin{bmatrix} C & D \\ T & E \end{bmatrix},$$

15 where C, D, E and T are matrices of appropriate dimensions and T matrix is upper-triangular. Such a form can be efficiently obtained by generalizing the approaches herein before described with reference to Figures 6 and 7

20 For example, if the approach herein before described with reference to Figure 6 is followed, then to generate an approximate triangular form, Step 1 remains the same, but the matrix H is now equivalently written in block-matrix form as

$$H = \begin{bmatrix} H_3 & H_4 \\ H_5 & H_6 \end{bmatrix},$$

25 where H_5 is a $tp \times tp$ matrix, with the integer $t \leq j$, and the matrices H_3 , H_4 and H_6 have appropriate dimensions. A triangularization step similar to Step 2 is applied to H_5 . Let U_5 be the $tp \times tp$ upper-triangular matrix obtained from H_5 by replacing each element on the main diagonal of H_5 with a 1 and by setting all the elements below the main diagonal to 0.

The $jp \times kp$ matrix

$$\begin{bmatrix} H_3 & H_4 \\ U_5 & H_6 \end{bmatrix},$$

5

is in approximate triangular form and therefore defines the parity-check matrix of a fast encodable LDPC code according to the aforementioned references D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Trans. on Communications*, Vol. 47, No. 10, pp. 1449-1454, Oct. 1999 and R. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. on Information Theory*, Vol. 47., No. 2, pp.638-656, Feb. 2001 . Step 3 then is applied to this approximate triangular matrix to eliminate possible 4-cycles.

10

Clearly, the matrix H in Step 1 can be rowwise and columnwise truncated to achieve specific values for the code word length and number of parity checks.

As indicated earlier, the approach herein before described with reference to Figure 7 can also be used to obtain a parity-check matrix in approximate triangular form. To this end, Step 1' is altered by cyclically shifting to the right the $t - 1$ lower block-rows of the matrix H^S . That is, the lowest block-row is shifted by $t - 1$ positions, the next upper block-row by $t - 2$ positions, etc. Then, Step 2' is applied, but only to the $tp \times tp$ lower-left submatrix of the so-obtained matrix, resulting in a new matrix with approximate triangular form. The overall matrix is then in approximate triangular form and free of 4-cycles and can directly be used for fast LDPC encoding following D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Trans. on Communications*, Vol. 47, No. 10, pp. 1449-1454, Oct. 1999 and R. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. on Information Theory*, Vol. 47., No. 2, pp.638-656, Feb. 2001 .

25

Again, the matrix obtained at the end of Step 2' can be rowwise and columnwise truncated to achieve specific values for the code word length and number of parity checks.

In some embodiments of the present invention, the parity check matrix may be defined by the matrix definition logic 300 upon connection of the transmitter 10 to the receiver via the communications channel 20. For example, the matrix may be built by the matrix definition logic 300 on connection based on dimensions negotiated between the endpoints of the channel 20. Specifically, the parity check matrix may be determined based on supply of the code parameter 170 to the transmitter 10 from the receiver 20. In other embodiments of the present invention, the parity check matrix may be defined by the matrix definition logic 300 in advance of a connection being established. For example, one or more parity check matrices may be preset within the matrix definition logic 300, with the or each preset matrix having a preset code length (number of columns) and a preset number of parity checks (number of rows). In embodiments having multiple preset matrices, an appropriate matrix is selected to the matrix definition logic 300 on establishment of the connection. Such a selection may be performed, for example, based on a negotiation between the endpoints of the channel 20 as herein before described.

Preferred embodiments of the present invention have been herein before described with reference to communications systems. However, the present invention is not limited in application to such systems. For example, referring to Figure 8, the embodiments of the encoder 110 herein before described may also be employed in a data storage system 210 for storing data from the information source 40 in a storage channel such as a hard disk storage channel.

It will be appreciated that the examples of the transmitter 10, encoder 110, and matrix generator 160 herein before described may each be implemented by hardwired logic, by a general purpose processor or dedicated digital signal processor programmed with computer program code, or by a combination of hardwired logic and computer program code. For example, referring to Figure 9, in the data communications system herein before described with reference to Figure 2, the transmitter 10 may comprise a programmable digital signal processor (DSP) 400 connected to a memory 410, with computer program code 420 stored in the memory 420 which, when executed

by the DSP 400, configures the DSP 400 to perform the steps of the method herein before described with reference to Figure 5.

While the invention has been described herein with reference to preferred embodiments, it will be appreciated by those skilled in the art that various changes in form and detail may be therein without departing from the scope of the invention.

5